Stealth Software Deters PHI Theft

Save to myBoK

by Terrance L. Kawles

As the leading edge of digital portability advances, the protections afforded the "portability" portion of HIPAA become strained. Under the final security standards, covered entities (CEs) must establish procedures and mechanisms to protect the confidentiality, integrity, and availability of electronic protected health information (PHI). The rule requires CEs to implement administrative, physical, and technical safeguards to protect electronic health information in their care.

This article will explore security issues related to portable devices as they relate to HIPAA.

Security on the Go

HIPAA makes no distinction between laptops, desktops, and personal digital assistants (PDAs). Moreover, the security regulations fail to address increased digital mobility and appear to presume that all computer hardware will be tied to a workstation in an office building.

For example, federal regulations require that all PHI be encrypted if it is sent over an open network, but they do not require hard disk encryption. The assumption seems centered around a basic premise that all hard disks reside inside desktop computers and as such are less likely to be compromised by theft.

Mobile devices, such as laptops and PDAs, enable the user to operate outside network defenses. Their portability makes them prime targets for theft, and if a laptop containing PHI files disappears, the CE violates privacy and security provisions in HIPAA.

Computer Theft Growing

The worldwide epidemic of computer theft is growing. According to Safeware, an insurance agency specializing in technology, more than 1,604,000 computers were stolen in the US in the last three years.[1] In 2002, 620,000 computers were stolen; in 2001, 591,000 computers were stolen; and in 2000, 387,000 computers were stolen. Worldwide statistics are proportionally similar.

These statistics should serve as a clarion call for CEs to reinforce protection measures. Loss of expensive hardware is bad enough, but once replacement cost is factored in, a pattern of computer loss can be catastrophic to HIPAA compliance plans. To help secure mobile technology, your organization should consider using theft deterrence or computer tracking applications.

Tracking Theft

Every time a CE computer with theft deterrence/computer tracking software connects to the Internet, the program sends a stealth e-mail message containing the computer's identity and its exact location anywhere in the world to a pre-determined e-mail address set by the CE. Once this information is received, recovery specialists from the software vendor work with the CE and the police to recover the stolen property.

To prevent removal of the tracking software, the program is highly tamper-proof and cannot be removed by unauthorized parties. The software is available both in single user and enterprise versions.

Theft Deterrence in Action

As the healthcare industry continues to tackle emerging security issues, it can look to other venues to benchmark security measures. For example, the Henrico County Public School District in Virginia implemented a program in 2001 to buy 23,000 laptop computers, which were to be distributed to every middle and high school student and teacher.[2]

As part of its theft-prevention and computer recovery program, Henrico County used theft deterrence/computer tracking software on the laptops. In its first year, the software performed as expected, providing Henrico with identification and location data necessary if any of the laptops were lost or stolen.

While the laptop program allowed students to keep the computers in their possession, Henrico did not experience a single case of theft or computer misplacement with the more than 12,000 computers in the initial rollout.[3] While it is difficult to provide empirical evidence to prove the reason for such non-events, it should be pointed out that Henrico, as part of its anti-theft policy, clearly informed the students and the public that it had the technical ability to track, locate, and retrieve any of the laptops should they be lost or stolen.

Given the circumstances, it is possible that the software's presence on the computers acted as a strong deterrent to potential computer thieves.

As advances in digital portability continue and the protections afforded PHI under HIPAA become even more vital due to the increasing use of mobile devices, it is important for a CE to consider tracking and encryption tools to assist with HIPAA compliance.

Notes

1. "Safeware's 2002 PC Loss Survey Shows Big Increase in Accidental Damage Claims." Press release, March 17, 2003. Available at www.assurant.com.
2. "Teaching and Learning Initiative." Henrico County (VA) Public Schools. Available at www.henrico.k12.va.us/ibook/index.html.
3. Internal data, Henrico County Public Schools and Brigadoon Software, Inc., fall 2002.

Reference

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. Federal Register 67, no. 157 (August 14, 2002). Available at http://aspe.hhs.gov/admnsimp.

Terrance L. Kawles *(tkawles@pcphonehome.com) is president of Brigadoon Software, Inc., and an attorney, entrepreneur, and expert in international, federal, and state surveillance and computer-based crime issues.*

Article citation:
Kawles, Terrance L. "Stealth Software Deters PHI Theft." *Journal of AHIMA* 74, no.7 (July/August 2003): 63-64.